REMOVABLE MEMORY, REMOVABLE MEMORY DRIVE AND SECURITY CONTROL METHOD

Patent Number: JP2001035092
Publication date: 2001-02-09
Inventor(s): SUGA KIMIHARU
Applicant(s): HITACHI MAXELL LTD
Requested Patent: JP2001035092
Application Number: JP19990201179 19990715
Priority Number(s):
IPC Classification: G11B20/12; G11B27/00
EC Classification:
Equivalents:

Abstract

PROBLEM TO BE SOLVED: To improve the security of stored information by setting and controlling the security data by employing the firmware of a removable memory drive of a removable memory. SOLUTION: Security data are controlled by the firmware of a removable memory drive 200 rather than the OS stored in a hard disk 340 of an external device 300. In other words, the device 300 can not make an access to a removable memory 100 unless a control section 210 discriminates the fact that the security data and a pass word are matched with each other. The possibility of making an access to the memory 100 by the drive 300 is determined without going through the OS of the device 300. Since no professional understands the firmware of the memory 200 unless he is the designer of the drive 200, the security of user's data is improved.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－35092
（P2001－35092A）
(43)公開日　平成13年２月９日(2001.2.9)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｇ１１Ｂ　20/12		Ｇ１１Ｂ　20/12		５Ｄ０４４
27/00		27/00		５Ｄ１１０
			Ｄ	

審査請求　未請求　請求項の数10　ＯＬ　（全 13 頁）

(21)出願番号　特願平11－201179

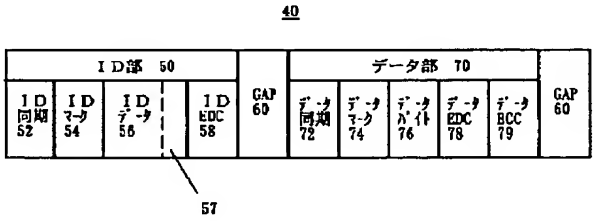
(22)出願日　平成11年７月15日(1999.7.15)

(71)出願人　000005810
日立マクセル株式会社
大阪府茨木市丑寅１丁目１番88号
(72)発明者　菅　君春
大阪府茨木市丑寅一丁目１番88号　日立マクセル株式会社内
(74)代理人　100110412
弁理士　藤元　亮輔

Ｆターム(参考)　5D044 BC01 CC04 DE02 DE48 DE52
5D110 AA13 DA01 DA12 DB02 DC11

(54)【発明の名称】　リムーバブルメモリ、リムーバブルメモリドライブ及びセキュリティ管理方法

(57)【要約】
【課題】　本発明は、格納された情報の機密性を従来よりも高めることができるリムーバブルメモリ、リムーバブルメモリドライブ及びセキュリティ管理方法を提供することを例示的目的とする。
【解決手段】　本発明のリムーバブルメモリはドライブのファームウェアによって設定及び管理されるセキュリティ領域を有している。このため、ドライブに接続されているオペレーションシステムではなく、ドライブのファームウェアによってリムーバブルメモリへのアクセスは管理される。



【特許請求の範囲】
【請求項１】　管理データを格納可能でユーザが書換え不能な管理領域と、
前記ユーザによる記録及び再生が可能なデータ領域と、セキュリティデータを格納可能なセキュリティ領域とを有するリムーバブルメモリであって、
前記セキュリティデータは前記リムーバブルメモリへのアクセスを制御するために前記リムーバブルメモリのリムーバブルメモリドライブのファームウェアにより設定及び管理されるリムーバブルメモリ。
【請求項２】　前記リムーバブルメモリはディスク状媒体である請求項１記載のリムーバブルメモリ。
【請求項３】　前記セキュリティ領域は前記ユーザがアクセス不能な領域に設けられている請求項１記載のリムーバブルメモリ。
【請求項４】　前記セキュリティ領域は前記リムーバブルメモリに複数点在している請求項１記載のリムーバブルメモリ。
【請求項５】　セキュリティ領域をリムーバブルメモリに形成するセキュリティフォーマットがユーザにより選択された場合に前記セキュリティ領域が存在することを表示するセキュリティフラグを設定して前記セキュリティ領域に格納する工程と、
ユーザが入力したセキュリティデータを前記セキュリティ領域に格納する工程とを有し、前記リムーバブルメモリのリムーバブルメモリドライブのファームウェアにおいて実行可能なセキュリティフォーマット方法。
【請求項６】　セキュリティ領域をリムーバブルメモリに形成するセキュリティフォーマットを選択するかどうかをユーザに要求する工程と、前記セキュリティフォーマットが前記ユーザにより選択された場合に前記セキュリティ領域が存在することを表示するセキュリティフラグを設定して前記セキュリティ領域に格納する工程と、前記ユーザにセキュリティデータを要求する工程と、前記ユーザが入力した前記セキュリティデータを前記セキュリティ領域に格納する工程とを有するユーティリティソフトウェアを格納した情報記録媒体。
【請求項７】　セキュリティ領域をリムーバブルメモリに形成するセキュリティフォーマットを選択するかどうかをユーザに要求する工程と、前記セキュリティフォーマットが前記ユーザにより選択された場合に前記セキュリティ領域が存在することを表示するセキュリティフラグを設定して前記セキュリティ領域に格納する工程と、前記ユーザにセキュリティデータを要求する工程と、前記ユーザが入力した前記セキュリティデータを前記セキュリティ領域に格納する工程とを有するユーティリティソフトウェアを通信回線を介して受信する受信部と、
前記ユーティリティソフトウェアを配信する送信部とを有する通信システム。
【請求項８】　管理データを格納可能でユーザが書換え不能な管理領域と、
前記ユーザによる記録及び再生が可能なデータ領域と、セキュリティデータを格納可能なセキュリティ領域とを有するリムーバブルメモリの前記セキュリティ領域をリムーバブルメモリドライブが読み出す工程と、
前記セキュリティデータとユーザが入力したパスワードとが一致するかどうかを前記リムーバブルメモリドライブが判断する工程と、
前記リムーバブルメモリドライブは、前記セキュリティデータと前記パスワードとが一致すると判断した場合に、前記管理領域を読み出して当該リムーバブルメモリドライブに接続された外部装置に前記管理データを伝達することによって前記外部装置が前記リムーバブルメモリにアクセスすることを可能にする工程と、
前記リムーバブルメモリドライブは、前記セキュリティデータと前記パスワードとが不一致であると判断した場合に、前記外部装置が前記リムーバブルメモリにアクセスすることを不能にする工程とを有する前記リムーバブルメモリのセキュリティ管理方法。
【請求項９】　管理データを格納可能でユーザが書換え不能な管理領域と、
前記ユーザによる記録及び再生が可能なデータ領域と、セキュリティデータを格納可能なセキュリティ領域とを有するリムーバブルメモリの前記管理領域をリムーバブルメモリドライブが読み出す工程と、
前記読み出し工程後に前記リムーバブルメモリドライブが前記セキュリティ領域を読み出す工程と、
前記セキュリティデータとユーザが入力したパスワードとが一致するかどうかを前記リムーバブルメモリドライブが判断する工程と、
前記リムーバブルメモリドライブは、前記セキュリティデータと前記パスワードとが一致すると判断した場合に、当該リムーバブルメモリドライブに接続された外部装置に前記管理データを伝達することによって前記外部装置が前記リムーバブルメモリにアクセスすることを可能にする工程と、
前記リムーバブルメモリドライブは、前記セキュリティデータと前記パスワードとが不一致であると判断した場合に、前記外部装置が前記リムーバブルメモリにアクセスすることを不能にする工程とを有する前記リムーバブルメモリのセキュリティ管理方法。
【請求項１０】　管理データを格納可能でユーザが書換え不能な管理領域と、　前記ユーザによる記録及び再生が可能なデータ領域と、セキュリティデータを格納可能なセキュリティ領域とを有するリムーバブルメモリを駆動すると共に外部装置に接続可能なリムーバブルメモリドライブであって、
前記リムーバブルメモリを再生可能なヘッドと、
前記ヘッドに接続されて当該ヘッドの出力を処理する信号処理装置と、

前記管理データと前記セキュリティデータとを管理可能なファームウェアを格納したメモリと、
前記ファームウェアに従って動作し、前記ヘッドが再生した前記セキュリティデータとユーザが入力したパスワードとが一致する場合に、前記外部装置が前記リムーバブルメモリにアクセスすることを可能にする制御装置とを有するリムーバブルメモリドライブ。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、一般に情報記録担体及びその駆動装置に係り、特に、ユーザが利用するユーザデータを格納する情報記録担体の前記ユーザデータへのアクセスを制御することを可能にするリムーバブルメモリと当該リムーバブルメモリを駆動するリムーバブルメモリドライブに関する。本発明は、例えば、映像情報、音声情報、テキスト情報、ソフトウェアなどを記録する光ディスク、光磁気ディスク、光サーボ方式を利用したフロッピーディスクなどのディスクにアクセスするためのセキュリティ情報を格納するディスク及びディスクドライブに好適である。また、本発明は、前記ディスク及びディスクドライブを利用したセキュリティ管理方法にも関する。かかるセキュリティ管理方法は、前記セキュリティ情報の生成、格納及び利用方法を含むものである。
【０００２】
【従来の技術】一般に、リムーバブルメモリとして、フロッピーディスク（ＦＤ）や光磁気（ＭＯ）ディスクなどの光ディスクや磁気ディスクなどが知られている。これらのディスクは、一般に、ユーザがアクセスできない管理領域とユーザがアクセス可能なデータ領域とを含んでいる。管理領域は、一般にディスクの制御情報、製造者情報、テスト情報などの管理データを格納しており、データ領域はユーザが利用することができる情報（以下、「ユーザデータ」という。）を格納している。
【０００３】従来のディスクは、典型的には、ディスクドライブが接続された外部装置（例えば、パーソナルコンピュータ）のオペレーションシステム（ＯＳ）上で管理されており、正当な権限を有しない者にアクセスされたくない情報（機密情報や著作物情報など）をディスクに記録する場合は、ＯＳ上からセキュリティをファイルやフォルダ毎にＯＳ上で起動するアプリケーションソフトウェアにより設定して情報へのアクセスを制限していた。アクセス制限は、ユーザデータの漏洩防止だけでなく、ユーザデータの改ざんと消去の防止をも目的にしている。セキュリティの設定及び実行においては、アプリケーションソフトウェアは、典型的に、ディスクドライブのヘッドがディスクから読み取ったデータ、パーソナルコンピュータのキーボードやマウスなどの入力手段を介してユーザが入力したデータ、パーソナルコンピュータのハードディスクに予め格納されているデータ、パーソナルコンピュータが接続されているモデムなどの通信回線を介して外部の認証機関から送信されるデータ、その他のデータ（例えば、指紋リーダや声紋リーダが読み取るバイオメトリックデータなど）からなるデータの一又は複数のデータを利用して、ユーザが正当な権限を有するものであるかどうかをパーソナルコンピュータの制御部が認証する。
【０００４】
【発明が解決しようとする課題】しかし、従来のＯＳを使用したセキュリティシステムは専門知識を有する者からユーザデータを保護するのに完全とはいえなかった。例えば、ＯＳによるセキュリティ管理はディスクコピーを可能にするため、専門知識を有する者は時間をかけてディスクに記録されたセキュリティデータを解析することができる。また、専門知識を有する者はアプリケーションソフトウェアを解析したり改ざんすることができ、セキュリティを突破することができる。更に、専門知識を有する者はディスクをドライブに挿入してＯＳを介さずに直接ユーザデータを読み出すことができる。
【０００５】
【課題を解決するための手段】そこで、本発明は、このような従来の課題を解決する新規かつ有用なリムーバブルメモリ、リムーバブルメモリドライブ及びセキュリティ管理方法を提供することを例示的な概括的目的とする。
【０００６】より特定的には、本発明は、格納された情報の機密性を従来よりも高めることができるリムーバブルメモリ、リムーバブルメモリドライブ及びセキュリティ管理方法を提供することを例示的目的とする。
【０００７】かかる目的を達成するために、本発明の例示的一態様としてのリムーバブルメモリは、管理データを格納可能でユーザが書換え不能な管理領域と、前記ユーザによる記録及び再生が可能なデータ領域と、セキュリティデータを格納可能なセキュリティ領域とを有し、前記セキュリティデータは前記リムーバブルメモリへのアクセスを制御するために前記リムーバブルメモリのリムーバブルメモリドライブのファームウェアにより設定及び管理される。かかるリムーバブルメモリによれば、セキュリティデータはリムーバブルメモリドライブに接続された外部装置のＯＳではなくリムーバブルメモリドライブのファームウェアによって設定及び管理される。
【０００８】本発明の例示的一態様としてのセキュリティフォーマット方法は、セキュリティ領域をリムーバブルメモリに形成するセキュリティフォーマットがユーザにより選択された場合に前記セキュリティ領域が存在することを表示するセキュリティフラグを設定して前記セキュリティ領域に格納する工程と、ユーザが入力したセキュリティデータを前記セキュリティ領域に格納する工程とを有し、前記リムーバブルメモリのリムーバブルメモリドライブのファームウェアにおいて実行可能であ

る。本発明の一側面はこのように従来は存在しなかったセキュリティ領域を物理フォーマットの一態様として形成している。従って、セキュリティフォーマットが施されたリムーバブルメモリはセキュリティフォーマットに対応可能なリムーバブルメモリドライブにおいてのみ駆動可能となる。

【０００９】本発明の例示的一態様としての情報記録媒体は、セキュリティ領域をリムーバブルメモリに形成するセキュリティフォーマットを選択するかどうかをユーザに要求する工程と、前記セキュリティフォーマットが前記ユーザにより選択された場合に前記セキュリティ領域が存在することを表示するセキュリティフラグを設定して前記セキュリティ領域に格納する工程と、前記ユーザにセキュリティデータを要求する工程と、前記ユーザが入力した前記セキュリティデータを前記セキュリティ領域に格納する工程とを有するユーティリティソフトウェアを格納している。また、本発明の例示的一態様としての通信システムはかかるユーティリティソフトウェアを、通信回線を介して送受信する送受信部を有する。かかる情報記録媒体及び通信システムは、上述のセキュリティフォーマット方法の作用を有するユーティリティソフトウェアを、媒体及び通信システムとして保護するものである。通信システムは、インターネット、専用回線その他の通信回線を介して不法に配信する一助をなすインターネットプロバイダー、商業サービスプロバイダーその他の通信業者が使用する通信システムをカバーするものである。

【００１０】本発明の例示的一態様としてのセキュリティ管理方法は、管理データを格納可能でユーザが書換え不能な管理領域と、前記ユーザによる記録及び再生が可能なデータ領域と、セキュリティデータを格納可能なセキュリティ領域とを有するリムーバブルメモリの前記セキュリティ領域をリムーバブルメモリドライブが読み出す工程と、前記セキュリティデータとユーザが入力したパスワードとが一致するかどうかを前記リムーバブルメモリドライブが判断する工程と、前記リムーバブルメモリドライブは、前記セキュリティデータと前記パスワードとが一致すると判断した場合に、前記管理領域を読み出して当該リムーバブルメモリドライブに接続された外部装置に前記管理データを伝達することによって前記外部装置が前記リムーバブルメモリにアクセスすることを可能にする工程と、前記リムーバブルメモリドライブは、前記セキュリティデータと前記パスワードとが不一致であると判断した場合に、前記外部装置が前記リムーバブルメモリにアクセスすることを不能にする工程とを有する。かかるセキュリティ管理方法によれば、リムーバブルメモリドライブによりセキュリティデータとパスワードとの一致があると判断されない限り外部装置はリムーバブルメモリにアクセスすることができない。

【００１１】本発明の別の例示的一態様としてのセキュリティ管理方法は、管理データを格納可能でユーザが書換え不能な管理領域と、前記ユーザによる記録及び再生が可能なデータ領域と、セキュリティデータを格納可能なセキュリティ領域とを有するリムーバブルメモリの前記管理領域をリムーバブルメモリドライブが読み出す工程と、前記読み出し工程後に前記リムーバブルメモリドライブが前記セキュリティ領域を読み出す工程と、前記セキュリティデータとユーザが入力したパスワードとが一致するかどうかを前記リムーバブルメモリドライブが判断する工程と、前記リムーバブルメモリドライブは、前記セキュリティデータと前記パスワードとが一致すると判断した場合に、当該リムーバブルメモリドライブに接続された外部装置に前記管理データを伝達することによって前記外部装置が前記リムーバブルメモリにアクセスすることを可能にする工程と、前記リムーバブルメモリドライブは、前記セキュリティデータと前記パスワードとが不一致であると判断した場合に、前記外部装置が前記リムーバブルメモリにアクセスすることを不能にする工程とを有する。かかるセキュリティ管理方法によれば、リムーバブルメモリドライブによりセキュリティデータとパスワードとの一致があると判断されない限り外部装置はリムーバブルメモリにアクセスすることができない。

【００１２】本発明の例示的一態様としてのリムーバブルメモリドライブは、管理データを格納可能でユーザが書換え不能な管理領域と、前記ユーザによる記録及び再生が可能なデータ領域と、セキュリティデータを格納可能なセキュリティ領域とを有するリムーバブルメモリを駆動すると共に外部装置に接続可能で、前記リムーバブルメモリを再生可能なヘッドと、前記ヘッドに接続されて当該ヘッドの出力を処理する信号処理装置と、前記管理データと前記セキュリティデータとを管理可能なファームウェアを格納したメモリと、前記ファームウェアに従って動作し、前記ヘッドが再生した前記セキュリティデータとユーザが入力したパスワードとが一致する場合に、前記外部装置が前記リムーバブルメモリにアクセスすることを可能にする制御装置とを有する。かかるセキュリティ管理方法によれば、リムーバブルメモリドライブによりセキュリティデータとパスワードとの一致があると判断されない限り外部装置はリムーバブルメモリにアクセスすることができない。

【００１３】本発明の更なる目的又はその他の特徴は添付図面を参照して説明される好ましい実施例において明らかにされるであろう。

【００１４】

【発明の実施の形態】以下、本発明の例示的一態様としてのリムーバブルメモリ１００について図１乃至図３を参照して説明する。リムーバブルメモリ１００は、磁気ディスク、光ディスク、光磁気ディスクなどを含むが、本実施例では、光サーボ方式を採用する磁気ディスク

（以下、単に「磁気ディスク」という。）をリムーバブルメモリ１００の例として説明する。図１に示すように、磁気ディスク１００は、管理領域１０ａ及び１０ｂとその間に存在するデータ領域４０とを有している。ここで、図１は本発明の例示的に光サーボ方式を採用する磁気ディスクとして具現化されたリムーバブルメモリ１００の平面図である。図１に示すように、ディスク１００は、周回方向に整列したトラックを有するデータ領域４０とグループ８０とを有している。ディスク１００は特徴的に光学式トラッキングサーボを採用し、グループ８０にレーザー光を照射して、グループ８０の有無によって変化する反射光の強弱を検出してトラッキングサーボを行い、例えば、２，４９０ｔｐｉの光トラック密度を実現している。グループ８０の数は、例えば、１６６６／周、９３０本／面、デューティー比５０％である。

【００１５】管理領域１０ａ及び１０ｂ（以下、特に断らない限り、参照番号１０はこれらを総括するものとする。）の各々は、図２に示すように、それぞれ、２つのディスク・メインテナンス・トラック（ＤＭＴ）２０ａ及び２０ｂ（以下、特に断らない限り、参照番号２０はこれらを総括するものとする。）を冗長的に有している。もっとも、本発明は管理領域１０ａと１０ｂがゼロ又は異なる数のＤＭＴ２０を有することを妨げるものではない。ここで、図２は、管理領域１０の構成を示す概略ブロック図である。ＤＭＴ２０はディスク・マッピング・トラック又はテーブルと呼ばれる場合もある。本実施例では、４つのＤＭＴ２０には同一のデータを冗長的に格納されているが、一又は複数のＤＭＴ２０は異なるデータを格納していてもよい。

【００１６】管理領域１０はユーザがアクセスできない領域である。「アクセスができない」とは、ユーザが通常のリムーバブルメモリドライブを使用した場合にはアクセスできないことを意味し、例えば、ユーザがドライブを改造したり、製造業者と同様の設備を用いた場合にも常に書換えが不能であるという意味ではないことに留意する必要がある。管理領域１０ａは、例えば、最初に後述するリムーバブルメモリドライブ２００のヘッド２３０がディスク１００をアクセスする領域であり、管理領域１０ｂは、例えば、読み終わりを示すバッファ領域であり、管理領域１０ａと対峙する最内周又は最外周に設けられている。

【００１７】表１に示すように、各ＤＭＴ２０は、一のセキュリティ・テーブル（ＳＴ）３０と、２つのＤＭＴセグメント２２及び２４を有している。ここで、表１はＤＭＴ２０の例示的な構造を示している。ＤＭＴセグメント２２及び２４は管理データを格納し、ＳＴ３０はセキュリティデータを格納する。また、表１において、ＳＴ３０はＤＭＴ２０内で先頭に配置されているが、これに限定されないことはいうまでもない。

【表１】

ＳＴ３０ ５１２バイト	バイト０	セキュリティ書込みカウント
	バイト１	セキュリティフラグ
	バイト２－３４	セキュリティドライブＳ／Ｎ
	バイト３	パスワードレングス
	バイト４	セキュリティレベル　１
	バイト５	セキュリティレベル　２
	バイト６	セキュリティレベル　３
	バイト７	セキュリティレベル　４
	バイト８	セキュリティレベル　５
	バイト９	セキュリティレベル　６
	バイト１０	セキュリティレベル　７
	バイト１１	セキュリティレベル　８
	バイト１２	セキュリティレベル　９
	バイト１３－１２７	リザーブド
	バイト１２８－１６４	セキュリティコード
	バイト１６５　ＦＦ	
	バイト１６６－５１１　０	
ＤＭＴセグメント２２ ５１２バイト	バイト０	ＵＳＮ
	バイト１－３	ＤＳＣ
	バイト４	ＲＳＣ
	バイト５－１２７	Ｆ
	バイト１２８－１３０	ＴＳＡゾーン０
	バイト１３１－１３３	ＴＳＡゾーン１
	バイト１３４－４５４	
	バイト４５５－４５７	ＴＳＡゾーン１０９
	バイト４５８－５１１　Ｆ	
ＤＭＴセグメント２４ ５１２バイト	バイト５１２－１０２１	再割当セクタ番号
	バイト１０２２－１０２３　Ｆ	

【００１８】管理データは、一般に、ディスク１００の制御情報、テスト情報、交替ブロック情報、不良セクタフラグ情報などを含んでいる。表１において、ＵＳＮは更新通し番号（Ｕｐｄａｔｅ　Ｓｅｒｉａｌ　Ｎｕｍｂｅｒ）、ＤＳＣはデータセクタカウント、ＲＳＣは再割当セクタカウント（Ｒｅａｓｓｉｇｎ　Ｓｅｃｔｏｒ　Ｃｏｕｎｔ）、ＴＳＡゾーンＸはゾーンＸにおけるトラックスタートアドレス、ＲＳＡは再割当セクタアドレス、ＬＢＡは論理ブロックアドレスを示している。

【００１９】セキュリティデータが格納されるＳＴ３０は広義にはセキュリティ領域に配置されると考えることができる。本実施例ではセキュリティ領域は管理領域１０内に設けられている。このように、セキュリティ領域はユーザがアクセスできない領域に設けられることが好ましい。これは、（１）本実施例のリムーバブルメモリ１００は書換え可能型であるためにセキュリティ領域が

データ領域４０に設けられれば誤ってユーザデータの書き込みに使用される場合があるのでこれを防止する必要があること、（２）ユーザが通常アクセスする領域ではなければ機密保持専用の領域として機能することが可能であることなどによる。但し、ユーザがアクセスできない領域は管理領域１０に限定されるものではない。例えば、データ領域４０内であってもユーザデータの記録再生に使用されない所定の目的用に予約された（リザーブド）領域をセキュリティ領域に割り当てることが可能である。従って、セキュリティ領域は管理領域１０の一部に限定されるものではない。

【００２０】ＳＴ３０は、ＳＴ３０の書き換え回数であるセキュリティ書込みカウント、セキュリティ領域の有無を表示するセキュリティフラグ、最後のセキュリティを加えたドライブ２００の通し番号を表示するセキュリティドライブＳ／Ｎを有している。パスワードレングスはセキュリティコードに格納されるべきパスワードの長さを表している。セキュリティコードは３６バイトを有して単純なアスキーコードを含む任意の暗号方法を利用して書き込まれることができる。１６５バイト目でセキュリティデータは終了するが、このバイトに限定されないことはいうまでもない。

【００２１】セキュリティ１乃至９には様々なセキュリティレベルを設定することができる。セキュリティレベル１は、例えば、ユーザが入力するパスワードと予めディスクに格納されているパスワードとの比較テスト回数が所定の回数を超えた場合にディスク１００をドライブ２００から排出する。セキュリティレベル２は、例えば、ユーザによるパスワード入力の失敗回数を定義し、規定回数を超えた場合にＤＭＴ２０を消去する。セキュリティレベル３は、例えば、セキュリティを加えたドライブ以外の読み出しを禁止する。その他のセキュリティレベルは更に付加的情報（ユーザ名、会社名、電話番号、バイオメトリックデータ、外部機関の認証コードなど）を要求することができる。

【００２２】セキュリティデータは、ＤＭＴ２０の数に応じて複数の箇所に物理的な距離を隔てて記録されている。複数の個所に記録される管理データの内容は同一及び／又は相違することができる。同一のセキュリティデータを複数の個所に冗長的に記録することはセキュリティデータの欠陥によるデータの損失を回避して信頼性を高める。例えば、図２に示す管理領域１０ａの２番目のＤＭＴ２０ａに格納されているセキュリティデータは最初のＤＭＴ２０ａに格納されているセキュリティデータの冗長であってもよい。特に、ディスク媒体は外周又は内周から錆により侵食されてデータが失なわれる危険性が高いので、セキュリティデータを冗長的に管理領域１０ａ及び１０ｂの両方に記録することが好ましい。

【００２３】本実施例においては、セキュリティ領域は、ディスクのフォーマット時にユーザがセキュリティフォーマットを選択した結果として形成される。ディスクの構造ではなく物理フォーマットのみを変更するだけであるため、本発明は従来のリムーバブルメモリ１００を使用することができる。本実施例では、各ＤＭＴ２０の先頭にＳＴ３０が配置されているが、ＳＴ３０の情報は、ばらばらに分割されて又は一括してＤＭＴセグメント２２及び２４の中に一個所に又は複数点在して配置されてもよい。

【００２４】相違する内容のセキュリティデータを複数の個所に記録することは全てのセキュリティデータを発見しないと意味のあるセキュリティデータが手に入らないことになるためにデータの信頼性を高める。必要があれば、各セキュリティデータのデータセグメントの結合方法に特徴があってもよい。例えば、管理領域１０ａにおいては図２に示す左から右に２つのＤＭＴ２０ａ内のセキュリティデータが結合され、管理領域１０ｂにおいては右から左に２つのＤＭＴ２０ｂ内のセキュリティデータが結合されるなどである。選択的に、いずれかのデータセグメントがその他の管理データセグメントの結合方法を定義していてよい。

【００２５】セキュリティデータはユーザデータへのアクセスを管理するのでユーザデータの機密保持を図る効果を有する。一般に、機密性（安全性）のレベルは、セキュリティデータが存在すること、及び、セキュリティデータの判別の困難性に依存する。機密性のレベルは一般にシステムが複雑であればあるほど高くなるが、複雑なシステムはコスト高を招き、信頼性の低下も招く。信頼性のレベルとコストは一般にシステムが単純であればあるほど高くなる。

【００２６】かかる問題を解決するために本実施例のセキュリティデータは基本的にはセキュリティフラグとパスワードのみを必須の構成要素としている。この結果、セキュリティデータの情報量をセキュリティデータの存在自体を発見されないほど少なくすることが可能である。セキュリティデータが発見されなければセキュリティデータは判別されず、また、その情報量が少なくければ単純にすることができる。セキュリティデータの機能を考慮すると、本実施例のセキュリティデータにはＩＳＯ標準光磁気ディスクの制御トラックのような従来の管理領域の情報量は不要である。もっとも、本発明はセキュリティデータのデータ量を増やすことを排除するものではない。

【００２７】また、本実施例ではセキュリティデータの記録領域をトラックの一部に限定しているのでセキュリティデータの存在を目立たなくするのに効果的である。従って、セキュリティ領域はディスク１００の全周（周回）に亘る必要がなく、ＳＴ３０を記録するのに必要充分な領域だけ確保すればよい。この結果、リムーバブルメモリ１００が光ディスクである場合にトラック毎にセキュリティデータの存在を判別しようとして顕微鏡など

で調べる悪意者は本実施例のディスク１００のトラックの一部のみを見てセキュリティデータは存在しないと判断するか、セキュリティデータの調査をあきらめるかもしれない。

【００２８】データ領域４０はユーザが利用できる領域であり、記録再生可能なディスク１００はこの領域を使用して映像情報、音声情報、テキスト情報、ソフトウェアその他の情報（ユーザデータ）を記録することができる。図３に、データ領域４０の例示的なセクターフォーマットの概略ブロック図を示す。なお、ディスク１００が再生されると、ヘッドはセクタを左から右に読んでいくものとする。

【００２９】図３に示すように、データ領域４０の各トラックは、ＩＤ部５０とギャップ６０とデータ部７０とを有している。ＩＤ部５０は物理フォーマット時にのみ形成され、ＩＤ同期部（ＩＤ　Ｓｙｎｃ）５２、ＩＤマーク５４、ＩＤデータ５６及びＩＤエラー検出コード（ＥＤＣ）５８を有している。ＩＤ同期部５２は、ＩＤマーク５４を見つけるためのハードウェアのための読み出し用トリガであり、ＩＤマーク５４はＩＤ部５０であることを識別する機能を有する。

【００３０】ＩＤデータ５６は対応するセクタのＩＤ（識別情報）を表しており、不良セクターフラグとしての情報を有すると共に、属性設定部５７を有している。ＩＤデータ５６は、例えば、７バイトの大きさを有しているが、従来においても２０ビット程度は使用されていなかった。属性設定部５７は、かかる未使用部を利用して設けられている。属性設定部５７は、対応するセクタの属性が読出し専用（リードオンリ）か書換え可能かを識別する。属性設定部５７が読出し専用と識別している場合には、データバイトフィールド７６のユーザデータが読出し専用になり、書換えができなくなる。ここで、「書換えができない」とは、ユーザが通常のディスク装置を使用した場合には書換え不能であることを意味し、例えば、ユーザがディスク装置を改造したり、製造業者と同様の設備を用いた場合にも常に書換えが不能であるという意味ではないことに留意する必要がある。また、属性設定部１７が読出し専用と識別している場合であっても、読出し自体を確保するために後述するＥＣＣ７９による誤り訂正は可能なように構成されることが好ましい。属性設定部５７が書換え可能と識別している場合には、データバイトフィールド７６のユーザデータは書換え可能にユーザに提供される。

【００３１】ＥＤＣ７８（又はこれに代替する機能的に類似のサイクリック冗長チェック（ＣＲＣ））は、ＩＤデータ５６が正しいかどうかを検出するがエラーの訂正はしない。選択的に、ディスク１００は、ＩＤ同期部５２の前に、セクタ同期部とセクタマークを更に有してもよい。

【００３２】ギャップ（Ｇａｐ）６０はセクタ間の緩衝を吸収する一種のバッファとして長さ調整のために挿入され、ＩＤ部５０とデータ部７０との間とデータ部７０とその次のＩＤ部５０との間に配置されている。

【００３３】データ部７０は、データ同期部（Ｄａｔａ　Ｓｙｎｃ）７２と、データマーク７４と、所定のデータ（ユーザデータ）７６と、データエラー検出コード（ＥＤＣ）７８と、データエラー訂正コード（ＥＣＣ）７９とを有している。データ同期部７２は、データマーク７４を見つけるためのハードウェアのための読み出し用トリガであり、データマーク７４はデータ部７０であることを識別する機能を有する。ユーザデータはデータバイトフィールド７６に格納され、例えば、エンドユーザ以外のメーカーが作成したＯＳ、ソフトウェアプログラム、画像情報、テキスト情報、音楽情報などのユーザが記録再生可能なデータなどの情報を含んでいる。データＥＤＣ７８は、ＥＤＣ５８と同様に、データバイトフィールド７６のユーザデータが正しいかどうかを検出するがエラーの訂正はしない。ＥＣＣ７９は、データバイトフィールド７６のユーザデータのエラー訂正を行って原データを復元することができる。

【００３４】本発明の光サーボ方式の磁気ディスク１００によれば、一枚のディスクの中に読出し専用な（即ち、ＲＯＭとして機能する）セクタと書換え可能な（即ち、ＲＡＭとして機能する）セクタとが混在することになる。また、属性設定部５７が格納されているＩＤ部５０はユーザには書換え不能な領域として構成されている。従って、ユーザはセクタの属性を自由に変更することができず、その結果、読出し専用に設定されたデータを変更することができない。ここで、「書換え不能」とは、ＩＤ部５０が、ユーザが通常のディスク装置を使用した場合には書換え不能であることを意味し、例えば、ユーザがディスク装置を改造したり、製造業者と同様の設備を用いた場合にも常に書換えが不能であるという意味ではないことに留意する必要がある。

【００３５】以下、リムーバブルメモリ１００と互換性のある本発明の例示的一態様としてのリムーバブルメモリドライブ２００の概略的な構成について図４を参照して説明する。ここで、図４は、リムーバブルメモリドライブ２００の概略ブロック図である。リムーバブルメモリドライブ２００は、本実施例ではパーソナルコンピュータとして具現化されている外部装置３００に接続された磁気ディスクドライブとして構成され、制御部２１０と、メモリ２２０と、ヘッド２３０と、信号処理装置２４０とを有している。その他、ドライブ２００は、図示しないボタンやキーボードなどの入力手段、液晶ディスプレイなどの表示手段を有することができる。

【００３６】制御部２１０は、メモリ２２０に格納されたファームウェアの制御の下、ヘッド２３０及び信号処理装置２４０の動作を制御する。ここで、「ファームウェア」は名称の如何を問わずメモリ２２０に格納されて

いるソフトウェアをいう。ファームウェアは、ディスク１００のフォーマットを行うユーティリティプログラムと、セキュリティ管理を行うセキュリティプログラムを含んでいる。

【００３７】ユーティリティプログラム及びセキュリティプログラムは、ドライブ２００の製造業者又は製造業者から委託をうけた業者から供給されるプログラムであり、後述されるリムーバブルメモリ（情報記憶媒体であればよい）３５２又は通信回線４３０を介してセットアップ、配信及びアップグレードなどが可能である。本実施例によれば、ユーザは通常フォーマットとセキュリティフォーマットを利用することができる。セキュリティプログラムは、正当な権限を有しないユーザがユーザデータのみならずディスク１００にアクセスすることを排除することを目的とするものである。ファームウェアの処理の詳細については後述する。

【００３８】ヘッド２３０は、ディスク１００の管理データ、セキュリティデータ及びユーザデータを読み出して、信号処理装置２４０に送信する。もっとも、後述するように、本実施例のヘッド２３０は、セキュリティデータがディスク１００に存在する場合には、メモリ２２０に格納されたファームウェアに従って制御部２１０の制御の下、セキュリティデータ又は管理データを最初に抽出して所定の処理を行った後に外部装置３００によるユーザデータへのアクセスを許容するため、管理データ、セキュリティデータ及びユーザデータが同時に信号処理装置２４０に供給されることはない。信号処理装置２４０は、外部装置３００のＳＣＳＩインターフェース３１２に接続されており、管理データ、セキュリティデータ及びユーザデータを復調して原情報を取り出すことができる。

【００３９】外部装置３００は、ＰＣＩバス３１０と、ＳＣＳＩインターフェース３１２と、ＩＤＥバス３１４と、メインメモリ３２０と、制御部３３０と、ハードディスクドライブ３４０と、リムーバブルメモリドライブ３５０と、リムーバブルメモリ３５２と、ディスプレイ３６０と、通信部３７０とを有している。なお、リムーバブルメモリ３５２と１００は同一で、リムーバブルメモリドライブ３５０と２００は同一でもよい。

【００４０】ＰＣＩバス３１０、ＳＣＳＩインターフェース３１２、ＩＤＥインターフェース３１４は当業界で周知であるのでここでは詳しい説明は省略する。メインメモリ３２０は、例えば、ＲＡＭやＲＯＭなどを含んでおり、制御部３３０の動作に必要なプログラムがハードディスク３４０から一時的にロードされたり図示しないキーボード、マウス、ジョイスティックなどの入力手段からの入力が一時的に格納されたり、システム動作に必要な情報を格納したりする。制御部３３０は各部の動作を制御し、ハードディスク３４０はウィンドウズ９８などのＯＳその他各部の動作に必要なプログラム（各種ドライバーなど）を格納している。リムーバブルメモリドライブ３５０とリムーバブルメモリ３５２は、ユーザデータに関連したした情報の記録再生に使用することができるが、本実施例では、ユーティリティプログラムのセットアップ及びアップグレードに使用される。ディスプレは、例えば、ＣＲＴディスプレイから構成される。

【００４１】外部装置３００は、更に、モデムなどの通信部３７０を有している。通信部３７０は、インターネット、アメリカ・オンラインなどの商業専用回線その他の回線からなる通信回線４３０を介して、更に外部装置５００に接続されている。通信回線４３０がインターネットであれば、より詳細には、外部装置３００は、契約しているインターネットサービスプロバイダー（の通信システム）４００と、外部装置５００が契約しているインターネットサービスプロバイダー（の通信システム）４１０を介して、外部装置５００と更新することができる。インターネットサービスプロバイダー（の通信システム）４００及び４１０は、周知の受信部４０２及び４１２と、送信部４０４及び４１４とを有している。

【００４２】以下、図５及び図６を参照して、リムーバブルメモリドライブ２００のセキュリティ管理について説明する。ここで、図５はリムーバブルメモリドライブ２００のセキュリティ管理の一例を説明するフローチャートであり、図６はリムーバブルメモリドライブ２００のセキュリティ管理の別の例を説明するフローチャートである。

【００４３】図５を参照するに、ディスク１００がドライブ２００に挿入されると、まず、制御部２１０はファームウェアに従ってヘッド２３０にＤＭＴ２０のＳＴ３０を読み出すように命令して（ステップ１００２）、セキュリティフラグが立っているかどうか（オンかどうか）を判断する。制御部２１０は、ディスク１００が挿入されたかどうかを、ドライブ２００に設けられてディスク１００の挿入を係合などの機械的手段やＬＥＤなどを利用した光学的手段などにより検出する検出部と交信することによって判断することができる。本実施例では、ディスク１００にはセキュリティフラグが立っていると仮定されているが、ドライブ２００は後述するセキュリティフォーマットを経たにも拘らずセキュリティフラグがたっていないディスク及び通常フォーマットを経たディスクにも互換性あるように構成することができる。かかる場合、制御部２１０は、セキュリティフラグが立っていない場合（オフの場合）又はＳＴ３０が存在しないと判断すると、後述のステップ１００８を実行することができる。

【００４４】さて、制御部２１０はセキュリティフラグが立っていると判断すると、「チェック・コンディション（Ｃｈｅｃｋ Ｃｏｎｄｉｔｉｏｎ）」と呼ばれる処理に移行する。チェック・コンディションはフラグがある場合のドライブ２００からのエラーコードである。こ

のエラーが発生した場合、ドライブ２００はそれ自体で、又は外部装置３００と協同して、ユーザにパスワードの入力を要求する（ステップ１００４）。ユーザへのパスワード要求はディスプレイ３６０にその旨を表示するか、ドライブ２００に設けられている液晶ディスプレイ、スピーカーその他の出力手段を利用して行うことができる。また、赤ランプや警告音などその旨を直接的に表現しなくてもよい。これに応答して、ユーザは、ドライブ２００に設けられているボタンなどの入力装置又は外部装置３００に接続されている図示しない入力手段（キーボード、マウスなど）を利用してパスワードを入力する。制御部２１０はセキュリティレベルに応じてパスワードと共に追加データの入力を促してもよい。この際、仮に専門知識を有する悪意者がセキュリティを解除しようとコマンドなどでアクセスしようとしてもモードセンス、モードセレクタなどで正確なパスワードを入力できなければ後述するようにディスク１００そのものへアクセスすることができなくなる。

【００４５】次いで、制御部２１０は、ＳＴ３０のセキュリティコードに予め格納されているセキュリティデータとユーザが入力したパスワードが一致するかどうかを判断する（ステップ１００６）。なお、「一致」とはパスワードとセキュリティコードが完全に同一であることを要求するものではない。例えば、セキュリティコードは許容されるパスワードの一覧表である場合があるからである。その場合には、その表に挙げられている一のパスワードを入力すればよい。必要があれば、ユーザデータ毎にセキュリティレベルを変更してセキュリティレベルの高いのデータには複数のパスワードを要求してもよい。制御部２１０は、セキュリティデータとパスワードが一致していると判断すれば管理領域１０のＤＭＴセグメント２２及び２４を読み出して管理データを信号処理装置２４０で再生してから外部装置３００にＳＣＳＩインターフェース３１２を介して送信する（ステップ１００８）。この結果、外部装置３００はディスク１００にアクセスしてユーザデータの記録再生を行うことができる。

【００４６】一方、制御部２１０は、不一致と判断すればユーザにパスワードの再入力を促して所定回数以内に一致しなければ、又は、不一致と判断すれば即座に、自動的にディスク１００をイジェクトする（ステップ１０１０）。より詳細には、ヘッド２３０がセキュリティデータをうまく読み取れなかった場合、読み取ったセキュリティデータが理解不能の場合、そしてユーザが入力したパスワードが正しくない場合にはエラー処理が行われる。エラー処理の場合にはディスプレイ３６０にその旨表示されて再試行などが促されるがいずれにしてもエラー処理においては信号処理装置３４０はユーザデータを再生することができない。これにより、ユーザデータの外部への流出を防止することができる。

【００４７】エラーが確定すれば制御部２１０はディスク１００をイジェクトする。所定回数のパスワードの入力が失敗したディスク１００は再度ドライブ２００に入力されても制御部２１０は直ちにエラーを確定してイジェクトすることができる。この結果、外部装置３００にはディスク１００に関して何の情報もドライブ２００から送信されなくなるので、制御部３３０はディスク１００が存在することすら認識できなくなる。

【００４８】代替的に、図６に示すように、管理領域を先に読み出して（ステップ１０１２）、その後にステップ１００２から１００４を行ってもよい。その後、制御部２１０は一致と判断すれば既に読み出した管理データを信号処理装置２４０で再生してから外部装置３００にＳＣＳＩインターフェース３１２を介して送信する（ステップ１０１４）。この結果、外部装置３００はディスク１００にアクセスしてユーザデータの記録再生を行うことができる。ステップ１０１２及び１０１４を採用する場合には、読み出した管理データはメモリ２２０その他の記憶部に一時的に格納することになるであろう。

【００４９】本発明の例示的一態様としてのセキュリティ管理方法によれば、セキュリティデータは外部装置３００のハードディスク３４０に格納されたＯＳではなくドライブ２００のファームウェアによって管理される。即ち、制御部２１０がセキュリティデータとパスワードの一致があると判断しない限り外部装置３００はリムーバブルメモリ１００にアクセスすることができない。外部装置３００のリムーバブルメモリ１００へのアクセス可能性は、外部装置３００のＯＳを介在しないで判断している。リムーバブルメモリドライブ２００のファームウェアはドライブ２００の設計者でなければ専門知識を有する者であっても理解することができないためにユーザデータの機密性を従来のＯＳによるセキュリティ管理方式よりも高めることができる。

【００５０】次に、図７を参照して、本発明の例示的一態様としてのフォーマット方法を説明する。ここで、図７は、リムーバブルメモリドライブ２００が実行するフォーマット方法を示すフローチャートである。まず、ユーザはドライブ２００にフォーマットされていない又は既にフォーマットされているディスク１００を挿入する。これに応答して、制御部２１０は、フォーマット形式の選択をユーザにステップ１００４などと同様に促す（ステップ１１０２）。

【００５１】なお、既にフォーマットがなされているディスクが挿入された場合、ユーザはドライブ２００に設けられているボタンなどの入力装置又は外部装置３００に接続されている図示しない入力手段（キーボード、マウスなど）を利用してフォーマット処理を選択する。既に通常のＯＳ（例えば、ウィンドウズ９８）に準拠してフォーマットされていれば、後述するステップ１１０４ではユーザはセキュリティフォーマットを希望すること

になるであろう。また、既にセキュリティフォーマットがなされていれば、後述するステップ１１０４ではユーザは通常のフォーマットを希望することになるであろう。セキュリティフォーマットが既にされていれば、ユーザは図５又は図６に示す処理を実行してパスワードその他の情報を入力することによって、外部装置３００によるリムーバブルメモリ１００へのアクセスを確保しておく必要がある。フォーマット形式を変更する場合には通常はユーザデータの消去を伴う。例えば、ＥＥなどの意味のないデータに変換することによって通常のノンセキュリティディスクとして使用することができる。しかし、代替的に、ユーザデータを消去しないでＤＭＴ２０のみを変更することができるであろう。

【００５２】次に、制御部２１０は、ユーザが入力したフォーマット形式が通常のフォーマットかセキュリティフォーマットかを判断する（ステップ１１０４）。ここで、「セキュリティフォーマット」とは、図３に示すＳＴ３０を形成する物理フォーマットをいう。ユーザが（クイックフォーマットを含む）通常のフォーマットを選択すれば（ステップ１１０４）、既知のフォーマット方法により管理領域とデータ領域が設定され、管理領域にはＳＴ３０を含まないＤＭＴが形成される（ステップ１１０６）。

【００５３】一方、ユーザがセキュリティフォーマットを選択すれば（ステップ１１０４）、制御部２１０は、管理領域１０とデータ領域４０が設定され、管理領域１０にはＳＴ３０を含むＤＭＴ２０が形成されることになる（ステップ１１０８）。この結果、ディスク１００は論理セキュリティディスクになる。なお、上述したように、ＳＴ３０はデータ領域４０に形成されても良いことに留意する必要がある。次に、制御部２１０はセキュリティフラグを立てる（ステップ１１１０）。より詳細には、セキュリティフォーマットが選択されてもユーザがパスワードを後述するステップ１１１２で入力しない場合には実質的に通常のフォーマットと同様であるとみなしてセキュリティフラグを立てないことも可能である。ユーザがパスワードを入力しなかったことはパスワードレングスにより判断することができる。代替的に、いかなる場合にもセキュリティフォーマットにおいてはパスワードを要求してセキュリティフラグを立ててもよい。

【００５４】次に、制御部２１０は、ユーザにパスワードその他に必要なオプションデータの入力（例えば、セキュリティレベルの設定、暗号の必要性、使用される暗号の種類、バイオメトリックデータの必要性、その他の付加的データ（ユーザ名、会社名、電話番号など）の必要性、外部認証機関からの認証の必要性）を促して、入力があるとこれを格納する（ステップ１１１２）。例えば、周知の暗号プロトコルをセキュリティデータに関与させることができる。例えば、リムーバブルメモリドライブに格納されるデータをオンライン（インターネットや商業オンライン回線など）により送信し、ディジタル署名とパブリック／プライベートキーを使用するなどである。

【００５５】このようにセキュリティフォーマットが施されたリムーバブルメモリ１００はセキュリティフォーマットに対応可能な専用のリムーバブルメモリドライブ２００においてのみ駆動可能となる。従って、仮にリムーバブルメモリ１００が盗まれても窃取者は専用のリムーバブルメモリドライブ２００を有していなければそれに格納されたデータを得ることができないため、ユーザデータの機密性は向上している。

【００５６】かかるセキュリティフォーマット方法はユーティリティソフトウェアとして、媒体（例えば、リムーバブルメモリ３５２）を介して、又は、通信システム４００及び４１０を介して、メモリ２２０のファームウェアにセットアップ及びアップグレードすることができる。

【００５７】図７には記載されていないが、ユーザは一旦設定したパスワードを変更することができる。また、パスワードを忘れてしまった場合に、所定の条件の下以前に入力されたパスワードを無効にすることも可能である。

【００５８】ドライブ２００は、ディスク１００の再生のみでなく記録も行うことができる。上述したように、ディスク１００は書換可能型であるためにユーザは以前のユーザデータに所望のデータを付加することができる。ディスク１００及びドライブ２００は、記録の際には、選択的に、追加的情報の入力と照合を行って再生時よりも機密性を高めてもよい。これにより、例えば、情報の一部が誤った情報に書き換えられたディスク１００が頒布されることを防止することができる。アクセスが許可・認証されたユーザにのみがユーザデータに記録をすることができるので以前に記録されたユーザデータが無防備に変更されることは防止される。リムーバブルメモリ１００は、例えば、病院の各患者毎の電子カルテ、保険会社の被保険者データ、企業の営業活動データ、公的機関の管理台帳などに使用することができる。

【００５９】以上、本発明の好ましい実施例を説明したが、本発明はこれらに限定されずその要旨の範囲内で種々の変形及び変更が可能である。例えば、本発明は、ディスクの種類（ＣＤ、光磁気ディスク、ＤＶＤなど）は問わない。

【００６０】

【発明の効果】本発明の例示的一態様としてのリムーバブルメモリによれば、リムーバブルメモリドライブのファームウェアはリムーバブルメモリドライブの設計者でなければ専門知識を有する者であっても理解することができないためにデータ領域に格納されたユーザデータの機密性を従来のＯＳによるセキュリティ管理方式よりも高めることができる。

【００６１】本発明の例示的一態様としてのセキュリティフォーマット方法によれば、セキュリティフォーマットが施されたリムーバブルメモリはセキュリティフォーマットに対応可能な専用のリムーバブルメモリドライブにおいてのみ駆動可能となる。従って、仮にリムーバブルメモリが盗まれても窃取者は専用のリムーバブルメモリドライブを有していなければそれに格納されたデータを得ることができないため、従来よりも格納されたデータの機密性は向上している。かかるセキュリティフォーマット方法はユーティリティソフトウェアとして、それを格納する媒体とそれを配信する通信システムを本出願において保護するものである。

【００６２】本発明の例示的一態様としてのセキュリティ管理方法によれば、リムーバブルメモリドライブによりセキュリティデータとパスワードの一致があると判断されない限り外部装置はリムーバブルメモリにアクセスすることができない。アクセス可能性を外部装置のＯＳを介在しないで判断しているために、上述のリムーバブルメモリと同様に、従来よりも格納されたデータの機密性は向上している。

【図面の簡単な説明】

【図１】　光サーボ方式を採用する磁気ディスクとして例示的に具現化された本発明の例示的一態様としてのリムーバブルメモリの平面図である。

【図２】　図１に示す磁気ディスクの管理領域の構成を示す概略ブロック図である。

【図３】　図１に示す磁気ディスクのデータ領域のセクターフォーマットを示す概略ブロック図である。

【図４】　図１に示すリムーバブルメモリと互換性のあるリムーバブルメモリドライブの概略ブロック図である。

【図５】　図４に示すリムーバブルメモリドライブが実行可能なセキュリティ管理の一例を説明するフローチャートである。

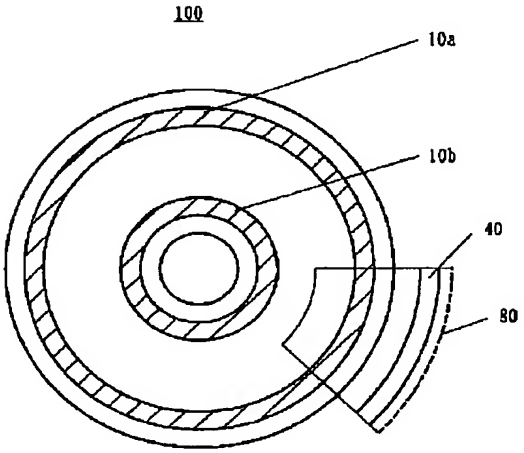
【図６】　図４に示すリムーバブルメモリドライブが実行可能なセキュリティ管理の別の例を説明するフローチャートである。

【図７】　図４に示すリムーバブルメモリドライブが実行するフォーマット方法を示すフローチャートである。

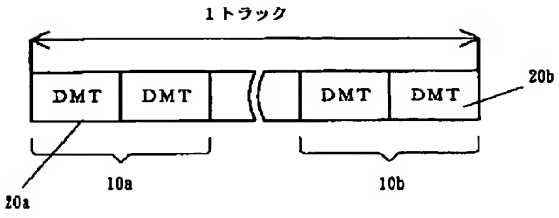
【符号の説明】

１００	リムーバブルメモリ
１０ａ	管理領域
１０ｂ	管理領域
２０ａ	ＤＭＴ
２０ｂ	ＤＭＴ
３０	セキュリティ・テーブル
４０	データ領域
５０	ＩＤ部
６０	ギャップ
７０	データ部
２００	リムーバブルメモリドライブ
２１０	制御部
２２０	メモリ
２３０	ヘッド
２４０	信号処理装置
３００	外部装置
３３０	制御部
３４０	ハードディスク（ドライブ）
３５０	リムーバブルメモリドライブ
３５２	リムーバブルメモリ（情報記憶媒体）
３７０	通信部
４００	通信システム
４１０	通信システム
４３０	通信回線

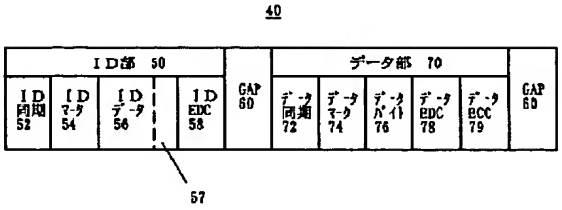
【図１】



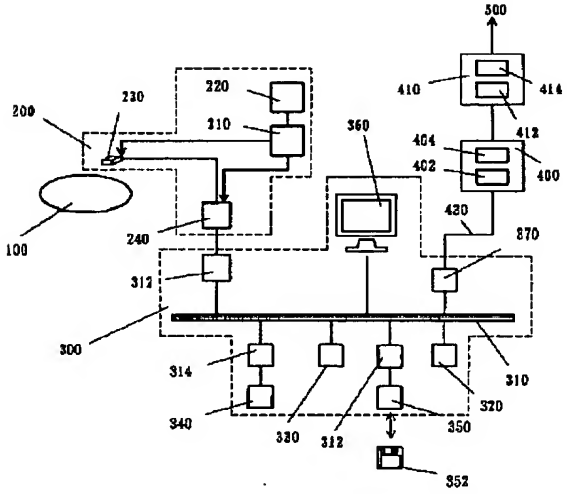
【図２】



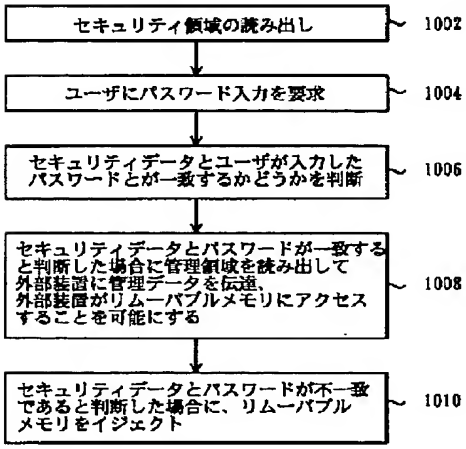
【図3】


40
ID部 50
データ部 70
ID同期 52
ID マーク 54
ID データ 56
ID EDC 58
GAP 60
データ同期 72
データ マーク 74
データ バイト 76
データ EDC 78
データ ECC 79
GAP 60
57

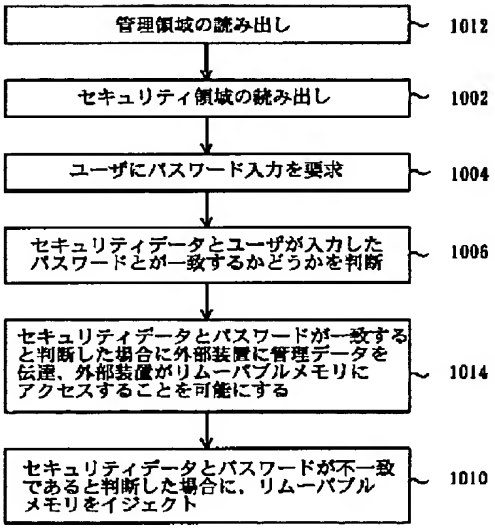
【図4】


500
410
414
412
404
402
400
200
230
220
310
360
420
870
240
100
312
300
314
310
320
340
330
312
350
352

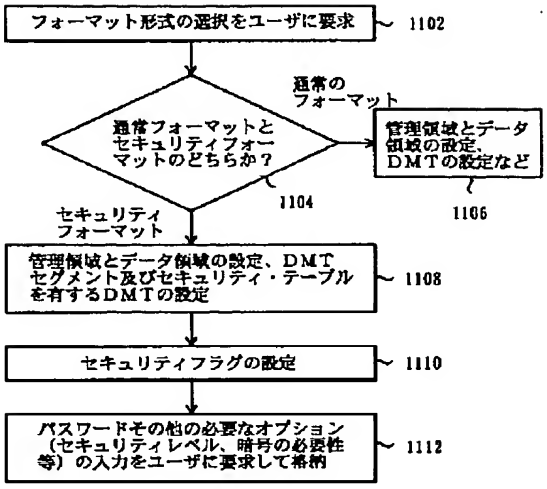
【図5】


セキュリティ領域の読み出し
1002
ユーザにパスワード入力を要求
1004
セキュリティデータとユーザが入力したパスワードとが一致するかどうかを判断
1006
セキュリティデータとパスワードが一致すると判断した場合に管理領域を読み出して外部装置に管理データを伝達、外部装置がリムーバブルメモリにアクセスすることを可能にする
1008
セキュリティデータとパスワードが不一致であると判断した場合に、リムーバブルメモリをイジェクト
1010

【図6】


管理領域の読み出し
1012
セキュリティ領域の読み出し
1002
ユーザにパスワード入力を要求
1004
セキュリティデータとユーザが入力したパスワードとが一致するかどうかを判断
1006
セキュリティデータとパスワードが一致すると判断した場合に外部装置に管理データを伝達、外部装置がリムーバブルメモリにアクセスすることを可能にする
1014
セキュリティデータとパスワードが不一致であると判断した場合に、リムーバブルメモリをイジェクト
1010

【図7】


フォーマット形式の選択をユーザに要求
1102
通常フォーマットとセキュリティフォーマットのどちらか？
1104
通常のフォーマット
管理領域とデータ領域の設定、DMTの設定など
1106
セキュリティフォーマット
管理領域とデータ領域の設定、DMTセグメント及びセキュリティ・テーブルを有するDMTの設定
1108
セキュリティフラグの設定
1110
パスワードその他の必要なオプション（セキュリティレベル、暗号の必要性等）の入力をユーザに要求して格納
1112